

REMARKS/ARGUMENTS

Favorable reconsideration of this application, as amended and in light of the following discussion, is respectfully requested.

Claims 1-18 are pending in this application. Claims 1, 4, 6, 11, 12, 15, and 16 are amended by the present amendment with support in the originally filed disclosure at least at Figures 5-8 and 17 and at paragraphs [0057], [0091], and [0093] to [0095] of the published Specification. Thus, no new matter is added.

In the outstanding Office Action, Claims 1-3 were rejected under 35 U.S.C. § 103(a) as unpatentable over Markham, et al. (U.S. Patent No. 7,231,664, herein "Markham") in view of Kadansky, et al. (U.S. Patent No. 6,295,361, herein "Kadansky"), and Claims 4-18 were rejected under 35 U.S.C. § 102(e) as anticipated by Markham.

Applicant respectfully traverses the rejections of the pending claims.

Response to Rejection under 35 U.S.C. § 103(a)

With regard to Claim 1, the outstanding Office Action asserts Markham as teaching every element except the element amended to recite "any terminal in the plurality of terminals is configured to perform the role of said first terminal and said second terminal," which it asserts Kakansky as teaching.

However, neither reference teaches or suggest "the **second terminal** is configured to **determine an end-terminal identifier in the broadcast frame as a broadcast address**, and **decode the payload of the broadcast frame using the broadcast encryption key assigned to the first terminal**," as recited by amended Claim 1.

Markham describes a **virtual private group, rather than an ad-hoc communication system**, as defined by Claim 1, in which nodes that are members of the same group share group security information. As shown at Fig. 3 and discussed at column 6, lines 23-47, of

Markham, a receiving node determines if a sending node is a member of its group and decrypts the send data using the group security information associated with its group only if the sending node is a member of its group. When the sending node is not a member of the receiving node's group, the receiving node processes the received data as plain text or discards the data, based on a policy established by an administrator of the virtual private group.

Markham does not discuss unicast or broadcast frames or different encryption keys based on the type of frame at all such that Markham does not teach or suggest a second terminal "configured to **determine an end-terminal identifier in the broadcast frame as a broadcast address**," as recited by amended Claim 1.

Kadansky fails to cure the deficiencies of Markham with regard to Claim 1.

Kadansky describes a multicasting group, rather than an ad-hoc communication system, as defined by Claim 1, in which a key manager node sets an indicator notifying all the nodes in the multicast group to change their key. However, Kadansky, like Markham, fails to teach or suggest a second terminal "configured to **determine an end-terminal identifier in the broadcast frame as a broadcast address**," as recited by amended Claim 1.

Because, even in combination, Markham and Kadansky fail to teach or suggest every element of amended Claim 1, the issue of the propriety of the combination is not even reached, and Applicant respectfully requests that the rejection under 35 U.S.C. § 102(e) of Claim 1 and Claims 2 and 3, which depend therefrom, be withdrawn.

Response to Rejection under 35 U.S.C. § 102(e)

The rejection of Claims 4-18 is addressed in detail below. At the outset, Applicant respectfully notes that, as set out in MPEP § 2131, "[a] **claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described,**

in a single prior art reference.” Verdegaal Bros. v. Union Oil Co. of California, 814 F.2d 628, 631. Further, “[t]he identical invention must be shown **in as complete detail as is contained in the...claim.**” Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1236.

If, upon considering the following arguments, the rejection based on Markham is maintained for any of Claims 4-18, Applicant requests a detailed articulation of the interpretation of Markham used to reject each claim.

Amended Claim 4 recites, *inter alia*, “an encryption-key management list table having at least one **encryption-key management list comprising a terminal identifier of a different terminal, a unicast encryption key between the terminal and the different terminal, and a broadcast encryption key assigned to the different terminal.**”

As described above, Markham is silent regarding “a **unicast encryption key between the terminal and the different terminal, and a broadcast encryption key assigned to the different terminal,**” as recited by amended Claim 4. Instead, Markham describes a group security information used for decryption of data from other members of the group of the receiving node. The group security information is not described as differentiating unicast and broadcast keys.

Because Markham does not teach or suggest at least the above-discussed features of amended Claim 4, Applicant respectfully requests that the rejection of Claim 4 under 35 U.S.C. § 102(e) be withdrawn.

Claims 11 and 15, though differing in scope and statutory class from Claim 4, patentably define over Markham for similar reasons as Claim 4. Thus, Applicant respectfully requests that the rejection of Claims 11 and 15 under 35 U.S.C. § 102(e) be withdrawn.

Claim 5 recites, *inter alia*, “an encryption-key management list table having at least one **encryption-key management list configured to store a unicast encryption key**

between said terminal and a different terminal and a broadcast encryption key assigned to the different terminal in association with a terminal identifier of the different terminal.”

The discussion with regard to Claim 4 is relevant to show that Markham, which describes a node in a virtual private group using group security information to decrypt data from another node in its same group, does not teach or suggest at least the above-quoted features of Claim 5 and, instead, is silent regarding storing both unicast and broadcast encryption keys altogether.

Thus, Applicant respectfully requests that the rejection of Claim 5 under 35 U.S.C. § 102(e) be withdrawn.

Amended Claim 6 recites, *inter alia*, “a **generated-key table configured to store a broadcast encryption key assigned to said terminal**, the broadcast encryption key being **different than a second broadcast encryption key assigned to a different terminal and also stored, in correspondence with the different terminal, in the terminal.**”

As is clear from the description of Markham above, only group security information common to the group of nodes is stored in a given node. Different security information associated with a second group, for example, is not stored in a node in a first group. Thus, Markham does not teach or suggest “**different...broadcast encryption key assigned to a different terminal and also stored, in correspondence with the different terminal, in the terminal,**” as recited by amended Claim 6.

Because Markham does not teach or suggest at least the above-discussed features of amended Claim 6, Applicant respectfully requests that the rejection of Claim 6 under 35 U.S.C. § 102(e) be withdrawn.

Claims 12 and 16, though differing in scope and statutory class from Claim 4, patentably define over Markham for similar reasons as Claim 4. Thus, Applicant respectfully requests that the rejection of Claims 12 and 16 under 35 U.S.C. § 102(e) be withdrawn.

Claim 7 recites, *inter alia*, “means for, **when a frame to be transmitted is a broadcast frame, encrypting** a payload of the broadcast frame **using the broadcast encryption key** of the generated-key table, **and when the frame to be transmitted is a unicast frame**, searching the encryption-key management list table for the encryption-key management list including a destination-terminal identifier of the unicast frame to encrypt a payload of the unicast frame **using the corresponding unicast encryption key.**”

As discussed with regard to Claims 4 and 5, Markham is silent regarding the use of a unicast encryption key for a unicast frame and a multicast encryption key for a multicast frame and, instead, describes group security information used for all communication among nodes in the same virtual private group.

Thus, Applicant respectfully requests that the rejection of Claim 7 under 35 U.S.C. § 102(e) be withdrawn.

Claim 8 recites “**means for encrypting a terminal identifier and a broadcast encryption key** of the terminal **using a unicast encryption key** assigned to a transmission-destination terminal; and means for transmitting the encrypted terminal identifier and broadcast encryption key of the terminal to the transmission-destination terminal.”

The outstanding Office Action cites portions of Markham, at page 8, without any information as to how the symmetric encryption algorithm or Encapsulating Security Payload header could teach or suggest the above-quoted features of Claim 8.

Because at least the highlighted features of Claim 8 are not taught or suggested by Markham, Applicant respectfully requests that the rejection of Claim 8 under 35 U.S.C. § 102(e) be withdrawn.

Claims 9, 13, 14, 17, and 18, though differing in scope and/or statutory class from Claims 5, 7, and 8, patentably define over Markham because they recite features directed to both a broadcast encryption key and a unicast encryption key which, as discussed with regard

to Claims 5, 7, and 8, are deficient in Markham. Accordingly, Applicant respectfully requests that the rejection of Claims 9, 13, 14, 17, and 18 under 35 U.S.C. § 102(e) be withdrawn.

Claim 10 recites “means for **receiving a terminal identifier and a broadcast encryption key of a different terminal** from the different terminal; means for **encrypting the terminal identifier and the broadcast encryption key of the different terminal using a broadcast encryption key assigned to the terminal**; and means for broadcasting the encrypted terminal identifier and broadcast encryption key of the different terminal.”

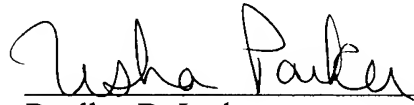
The discussion of Claim 10 at page 9 of the outstanding Office Action does not address the above-highlighted features at all. The “decrypting the encrypted data packet” noted in the outstanding Office Action would necessarily use the same group security information asserted for the feature of “encrypting...using a broadcast encryption key assigned to the terminal.” More significantly, Markham’s “receiving secure data,” which appears to be asserted as teaching “receiving a terminal identifier and a broadcast encryption key of a different terminal,” as recited by Claim 10, is not described as including a broadcast encryption key of a sending node at all. The basis for the rejection of Claim 10 is entirely unclear.

Because Markham fails to teach or suggest at least the above-highlighted features of Claim 10, Applicant respectfully requests that the rejection of Claim 10 under 35 U.S.C. § 102(e) be withdrawn.

Accordingly, the outstanding rejections are traversed and the pending claims are believed to be in condition for formal allowance. An early and favorable action to that effect is, therefore, respectfully requested.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

A handwritten signature in dark ink, appearing to read "Usha Parker", is written over a horizontal line.

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413-2220
(OSMMN 08/07)

Usha Munukutla-Parker
Registration No. 61,939